NHII ADVISORS
1854 CLARENDON BLVD.
ARLINGTON, VA 22201
703/527-5678

WILLIAM A. YASNOFF, MD, PHD
MANAGING PARTNER
WILLIAM.YASNOFF@NHIIADVISORS.COM

12/4/05

Electronic Records in Health Care: The Problem and the Solution

The Problem of Electronic Records in Health Care

While the U.S. health care system is capable of delivering superb medical care, it is also plagued with inconsistent quality, unreliable safety, and escalating costs. All of these problems are largely traceable to the lack of availability of complete patient information resulting from continuing dependence on paper records. The intelligent application of modern information technology to health care has long been recognized as a critical and urgent need – according to the Institute of Medicine, it should be "the highest priority for all health care stakeholders"[1] The plain fact is that "paper records kill" – and we have the technology for electronic medical records that would fix the problem.

Despite widespread agreement on the need for action at the community level to address this urgent and critical issue, progress has been very slow toward widespread and consistent use of health information technology. Obstacles include misaligned incentives, lack of medical information standards, and no clear source of funding for this new activity. Any proposed solution must provide for the availability of complete patient information while assuring universal cooperation of the diverse health care stakeholders, ongoing funding for sustainability, and the high level of public trust needed to operate a system that is responsible for extremely sensitive medical information in electronic form on behalf of the everyone in the community.

Complete patient information is the first key requirement. While much of existing health care information is already electronic (e.g. labs and medications), and some hospitals have electronic health record (EHR) systems, over 85% of office-based based physicians still rely solely on paper records. In order make complete patient records rapidly available, all such records must be electronic. Therefore, office-based physicians must obtain and use EHRs. However, since most of the benefits of EHRs in the ambulatory setting accrue to others (besides the practice acquiring the system), financial incentives must be available to office-based practitioners for EHRs.

---

[1] Institute of Medicine. Committee on Data Standards for Patient Safety. *Patient Safety: Achieving a New Standard for Care.* Washington, DC: National Academy Press, 2003.

Universal cooperation of health care stakeholders is essential. Since most patients obtain their care from multiple sources, their medical information is scattered in various systems. There must be incentives for collecting and collating each patient's information and making it available when and where needed. Existing efforts to share patient information electronically have been slowed and even stymied by disagreements related to the terms and conditions of information exchange. A strategy must be developed to ensure that all holders of patient information will make it available.

Ongoing funding is essential for the success of a health information system. Naturally, it is extremely difficult to engage the cooperation of stakeholders to create a system in the absence of a clear path toward financial sustainability. Although a comprehensive system of electronic medical records will benefit all health care stakeholders, the specific allocation of the costs has proven to be a formidable (and usually insurmountable) barrier to progress. The well-established tradition in health care of shifting costs to other stakeholders has made this problem especially difficult. Any potential solution must present a sufficiently strong value proposition (in advance) to assure the long-term financial viability of the system.

Finally, public trust is essential to any effort to facilitate access to complete electronic medical records. The public correctly perceives that any efforts to make medical records more accessible for appropriate and authorized purposes simultaneously carry the risk of increased availability for unscrupulous use. Therefore, stringent privacy and confidentiality policies enforced with effective security measures are needed to protect sensitive medical information. The trust of the public is an essential prerequisite for any organization implementing such measures so as to responsibly function as the medical records custodian for the community. Allowing patients to completely control all access to their records is an important component of earning such trust. Consumer participation in the organization at the highest levels, open and transparent management, and independent ongoing review of privacy practices and complaints are also needed. All these elements must be part of any proposed solution.

Until now, there has not been a specific, feasible, and understandable path that addresses the key issues of complete information while assuring stakeholder cooperation, ongoing funding, and public trust. Although progress has been made, and a few communities even have very advanced systems that deliver partial medical information, no community has yet succeeded in creating a system that provides complete patient information. This document presents a proposed solution to these difficult problems, known as an eHealthTrust.

A Solution for Electronic Records in Health Care: eHealthTrust™

The eHealthTrust makes complete patient information available when and where needed by serving as the community custodian of the complete medical records for everyone (since health care is a community-based activity, it is a community-based approach). Each person controls all access to his/her records, and is charged about $60/year ($5/month) for the service (which may be [and should be] reimbursed as an allowable

medical expense).[2] The eHealthTrust pays physicians $2-4 for the "deposit" of each standardized electronic report of an outpatient encounter, thereby creating potential new revenue of $10-20,000/year for physicians with EHR systems (thereby providing the needed incentives for their acquisition and use). Since the patients explicitly provide consent for the eHealthTrust record keeping activities, cooperation of all health care stakeholders in providing information is assured (since medical records must be provided on patient request under the Federal HIPAA statute). The eHealthTrust model assures public trust by putting the patient in control of his/her information. While ongoing funding is assured through continued patient payments, startup funding to begin an eHealthTrust must be separately obtained.

The eHealthTrust provides a specific, feasible, and understandable path that clearly leads to the availability of complete electronic patient information while assuring stakeholder cooperation, ongoing funding, and public trust. What follows is a detailed description of the eHealthTrust divided into nine sections: I. Overview; II. Information Flow; III. Standards and Interoperability; IV. Organization and Governance; V. Privacy; VI. Technical Architecture; VII. Benefits to Stakeholders; VIII. Financial Considerations for Startup; and IX. Risks and Mitigation Strategies.

I. Overview of eHealthTrust

a. Custodian of lifetime medical records of members[3] on their behalf
b. All access to records controlled by members (or their proxy)
c. Modest fees (~$60/year) paid by patients
    i. May be reimbursed by health plans/employers
d. Scope is community or region (may be state)
e. Suppliers of standard electronic medical record information paid
    i. Clinicians receive $2-4/encounter for electronic reports (provides incentives of $10-20,000/ clinician/year for acquiring and using EHRs)
    ii. Other medical record suppliers paid small per record fee
f. Cooperation of holders of medical record information assured by HIPAA requirement to provide records on patient request

II. Information Flow

a. Enrollment & initial collection of records
    i. Member provides demographic information, list of medical providers
    ii. Member specifies standing instructions for allowable access to records; default includes
        1. unlimited access by listed providers
        2. emergency access by bona fide emergency provider

[2] A national survey sponsored by Accenture in May, 2005, showed that 52% of consumers were willing to pay at least $5/month for electronic records (see http://www.accenture.com/xd/xd.asp?it=enweb&xd=_dyn%5Cdynamicpressrelease_857.xml)
[3] interchangeably referred to as subscribers, consumers, or patients in this document

3. notification to member of clinical trial eligibility (no other party notified)
4. access to de-identified data for research, with bulk of fees for research access credited back to the member

iii. Member receives ID card; returns signed consent
1. ID is like credit card – number links to member account
2. Access to record requires ID card and prior patient permission

iv. Listed providers contacted on behalf of member (per consent form) with request to provide information ("initial deposit")
1. Discharge summaries requested from hospitals
2. Complete test results requested from laboratories
3. Image interpretation reports requested from imaging centers
   a. Electronic linkage established to original images, which remain in their current location (not copied to eHealthTrust)
4. Medication history requested from Pharmacy Benefit Manager (PBM) or Prescription clearinghouse
5. Office-based clinicians asked for synopsis of records: problem list, allergies, most recent complete physical, notes from 2 most recent encounters
   a. If no EHR: fax paper copies to eHT, images stored
   b. If EHR: send electronic information (in standard format TBD – could be CCR [continuity of care record])
6. Claims information could optionally be included

b. Access to individual records
i. Via secure web portal
1. Member interface allows
   a. Viewing complete record (no changes to record allowed)
   b. Management of access permissions
2. Member interface may also include capability to
   a. Add information (personal health record)
   b. Communicate securely with clinicians (e-mail)
   c. Access authoritative health & health care information
   d. Receive customized reminders and health alerts
3. Clinician interface includes clinically relevant information display tools

ii. If clinician has no web access, member brings printed copy of records to encounter

c. Adding new medical record information ("ongoing deposits")
i. Office clinicians send notes from each encounter
1. Via fax if paper record

a. Minimal reimbursement optional (e.g. 10¢)
2. In standard electronic form from EHR
a. Reimbursement of $2-4 for each record sent

ii. Other record generators send new records when produced
1. Hospitals send new discharge summaries
2. Laboratories send new results
3. PBMs send new prescriptions
4. Imaging centers send new reports

iii. New records relating to members of other eHealthTrusts (who receive care while visiting community)
1. Intercepted by "clearinghouse server" at eHealthTrust
2. Routed directly to proper eHealthTrust

d. Public health reporting
i. All incoming records (except faxes) reviewed for public health reportability
ii. Copies of reportable events transmitted to public health agency
iii. Can substitute for direct reporting (benefit to clinicians and other entities responsible for public health reporting)

e. Access to records for research
i. Requires patient consent
ii. Requires Institutional Review Board (IRB) approval
iii. No identified data is returned to researchers
iv. Message from researcher may be delivered to members meeting specific criteria (i.e. to recruit volunteers for a clinical trial)
v. Fees charged to researchers; bulk of proceeds credited to members

III. Standards & Interoperability

a. All entities in community have single interface to eHealthTrust
b. eHealthTrusts have no need to communicate with each other to retrieve records (since each person's entire record is in a single eHealthTrust)
i. new records from visitors to community who receive care are routed to their "home" eHealthTrust by "clearinghouse server" at each eHealthTrust

c. Interoperability standards set by eHealthTrust Association
i. All eHealthTrusts must have license to eHealthTrust business process patent (covering payments by an eHealthTrust to clinicians for depositing patient information)
ii. Patent license requires membership in eHealthTrust Association & adherence to its standards (licensing fees are minimal)

d. Initial standard for transmitting outpatient encounter data will be as recommended by EHR Vendors Association
i. One standard needed for all eHealthTrusts so vendors can market HIT systems nationwide with a uniform interface

e. Gradual improvement of standards over time
i. Initial standards will have many "free text" fields

ii. Standard encoding of all fields will be promoted with eHealthTrust reimbursement policy
    1. Future encoding requirements will be announced with substantial lead time for implementation (e.g. 2 years)
    2. Ongoing reimbursements will provide funds for needed system upgrades
    3. Future reimbursement will require compliance with scheduled encoding requirements
iii. Provides for greater use of encoded information over time (e.g. for decision support)

IV. Organization & Governance

a. New non-profit organization to maximize participation and public trust
    i. Board has representation from all stakeholders (consumers, clinicians, health care organizations, payers, employers, government)
    ii. Consumers have substantial voice
    iii. Open and transparent deliberations
    iv. Public financial disclosure
    v. Independent privacy audit committee (of Board) with authority to
        1. investigate privacy violations
        2. recommend sanctions
        3. recommend policy changes
b. Policies and procedures established by non-profit
c. Operations by for-profit contractor or subsidiary
    i. Specifications and performance criteria established by non-profit
    ii. For-profit operations model facilitates capital acquisition by providing ROI
    iii. Operations entities may serve multiple eHealthTrusts
d. Functions of eHealthTrust Association
    i. Provide license for business process patent
    ii. Provide software for "clearinghouse server"
        1. Checks incoming messages for standards compliance
        2. Sends copies of reportable information to public health
        3. Routes incoming messages for members of other eHealthTrusts to their "home" eHealthTrust
    iii. Facilitate research queries across multiple eHealthTrusts
        1. Arrange for distribution of queries and aggregation of results
        2. Distribute fees from researchers to eHealthTrusts
    iv. Update & maintain information exchange standards
        1. Common function for all eHealthTrusts
        2. Add new terms; update codes

V. Privacy

a. Key principle: no information is released without member consent

b. Consent may be restricted to
    i. Specific time periods (e.g. access to a specialist for a specific condition lasting a few months)
    ii. Specific information (e.g. access to testing for sexually transmitted diseases can be "suppressed" by the member)
c. Research access to data by consent
    i. No patient identifying information released
    ii. Permission requests for release of needed information may be sent to selected patients on behalf of researchers
d. Information transferred to another eHealthTrust on member request (to transfer membership)
e. Information returned to member and erased on request (to terminate membership)
f. Employees of eHealthTrust must be carefully screened
    i. Extensive background checks
    ii. Strict confidentiality agreements
    iii. Consistent and immediate sanctions for violations
g. Physical security
    i. Operating site must have extensive physical security
        1. Information highly sensitive and valuable
        2. Operations center is highly visible & known target
        3. Need to deter break-in/theft
    ii. Fencing/security guards/alarms
    iii. Protection level similar to high-security government facility

VI. Technical Architecture

a. Separate clinical and research servers
    i. Clinical server provides complete patient records, but does not permit searching
    ii. Research server allows searching, but has no phone or Internet connections (for security)
b. Clinical server details
    i. "Cubbyhole" server only retrieves a single complete record
        1. other functions not present
        2. user "logged off" after retrieving one record
    ii. Uses highly secure, separation kernel operating system (see Rushby, Proceedings of the eighth ACM symposium on Operating systems principles (1981); e.g. http://www.lynuxworks.com/rtos/secure-rtos-kernel.php)
        1. Each user has own "virtual machine"
        2. Cannot affect any other user
    iii. Initial implementation with secure Linux (see http://www.nsa.gov/selinux/index.cfm)
    iv. Secure, encrypted Internet access
        1. 128-bit SSL encryption (via browser)
        2. secure authentication (specifics TBD by each eHealthTrust)

a. may include digital certificate/token/biometric ID for health care professionals

3. access to member record by authenticated health care professional requires both
    a. specific member permission (via secure online access or 800-number in emergency)
    b. member ID number (provided by member)

c. Research server
    i. No phone or Internet connections (to prevent unauthorized access)
    ii. Standard operating system & database software
    iii. Specific permissions from members for various categories of research restricts queries (categories may include notification of product withdrawal, clinical trials, public health, medical research, etc.)
    iv. All queries submitted in machine room by operations personnel
    v. Results (non-identified) encrypted for transmission back to researchers
d. Backup & disaster recovery
    i. Clinical server is highly redundant & reliable design with internal component duplication for high availability (i.e. dual processor, mirrored RAID disk drives, UPS, standby backup power, etc.)
    ii. All information backed up on site (research server) and at two other separate geographic locations
    iii. Immediate capability to switch to backup server in case of failure
    iv. Potential for reduced cost backup capability through "mutual aid" agreements with other eHealthTrusts

VII. Benefits to Stakeholders

a. Members (consumers)
    i. Complete medical records with access & control
    ii. Improved quality of care; reduced errors
    iii. Lower cost of care
    iv. Customized information about health (e.g. recommendations and reminders)
    v. More medical research → better treatments
    vi. Modest fees ($5/month); may be covered by sponsor (e.g. employer)
b. Clinicians
    i. Access to complete medical records → better care
    ii. Financial incentives for EHRs
c. Employers (including government)
    i. Lower cost, higher quality care
    ii. Estimated savings of 8% of health care costs
d. Health care institutions
    i. Access to complete medical records → better care
    ii. Improved efficiency (e.g. avoid duplicate tests)

iii. More opportunities for research

e. Government
   i. Lower cost, higher quality care
   ii. Reduced growth of Medicare & Medicaid expenditures
   iii. Better information at lower cost for public health
   iv. Lower cost of medical research

f. Payers
   i. Lower cost, higher quality care
   ii. Information available to monitor quality (with member consent)

VIII. Financial Considerations for Startup

a. Phase I – no EHR incentives
   i. Advantages of delaying EHR incentives
      1. EHR incentives require intensive local marketing to be successful (which is expensive)
         a. A significant percentage of patients in a clinician's practice must be eHealthTrust members for incentives to be effective (e.g. 70-80%)
         b. Otherwise total incentive is too small (e.g. if 10% of practice, incentive would only be $1,000-2,000/yr)
      2. Saves the money that would be paid as incentives in the initial rollout, reducing the cost/time to breakeven (and the initial investment needed)
      3. Delay does not cause serious problems
         a. eHealthTrust has substantial value without EHR incentives
         b. even with incentives, will take time for clinicians to acquire EHR systems
            i. Phase I delays this a bit longer (months)
   ii. Phase I eHealthTrust is marketed to large population (e.g. state with population of 5 million)
      1. Large marketing area possible if no EHR incentives
         a. Intensive local activity not necessary
      2. Very modest market penetration needed to break even
         a. Survey in May 2005 indicated that 52% of consumers were willing to pay $5/month or more to have electronic medical records (see p. 3 footnote)
         b. Only need 100,000 members to break even (2% of 5 million)
   iii. Use proceeds of statewide rollout to fund Phase II
      1. After breakeven, margins exceed 90%
      2. Membership of 150,000 generates $3 million per year in "profit"
      3. Invest "profit" in rollout of Phase II in one community at a time (or in stages)

4. After high penetration achieved in initial Phase II area, move to next area
5. Result is complete eHealthTrust in entire state with single initial investment

iv. Initial investment
1. Depends on
a. Fixed startup costs
i. Hardware (~$500,000)
ii. Software (~$500,000)
iii. Staff costs prior to breakeven
iv. Help desk costs prior to breakeven
b. Time to breakeven
i. Depends on rate of member acquisition
ii. Large initial group of subscribers (80,000) results in rapid breakeven (2 months)
2. Varies from $2.6 million to $4.4 million depending on member acquisition rate:

Subscribers/month	breakeven time	investment
25,000	4 months	$3 million
16,667	7 months	$3.4 million
12.500	8 months	$3.7 million
8,333	12 months	$4.4 million
8,333+80,000 at start	2 months	$2.6 million

3. Is reduced substantially if there is a guaranteed initial customer base commitment
a. Eliminates uncertainty about speed of acquiring subscribers (market risk)
b. Ensures almost immediate breakeven

b. Phase II – add EHR incentives in one community (population 1,000,000)
i. Select community most likely to be successful
1. Strong support of clinicians
2. All employers agree to cover full cost for their employees ($60/year)
3. Strong support of government officials
4. Extensive coverage promised by local media
ii. Proceeds of Phase I allow complete EHR incentives from start
1. Clinicians immediately receive payment for every standard electronic report of an encounter for all their patients
a. Records for eHealthTrust members put in repository
b. Other patient records put in "backup" storage – not accessible until those patients become members
c. Results in immediate strong incentives for EHR adoption
2. Can also pay bonus to physicians enrolling their patients
a. $10 payment to physician for each patient referred who joins eHealthTrust

b. can split this bonus with patient to provide "discounted enrollment" at physician offices

iii. Effectiveness of EHR incentives depends on rate of penetration of community
1. When 250,000 enrollees (25% penetration) in first community, net "profits" are back up to annual rate of $3 million
2. Can then begin next community

iv. Takes 5 iterations of Phase II (e.g. five years) to cover communities including all 5,000,000 people in the state
1. Conservative assumptions lead to 1.5-2 million eHealthTrust members in about 6 years
2. Could grow more rapidly
3. Once "critical mass" is reached, adoption rate may accelerate

c. Special populations

i. Medicaid
1. State commitment to enrolling Medicaid recipients immediately greatly reduces needed investment, & startup risk
2. Potential substantial savings to state in health care costs
a. eHealthTrust costs about 1% of health care costs
b. estimated benefits are about 8% of health care costs
3. In a typical state with a population of 5 million with 14% Medicaid recipients, total cost for the eHealthTrust would be $42 million/year (700,000 recipients x $60 each). This represents 1% of total Medicaid spending and about 2.4% of state Medicaid spending. The potential annual health care savings (8%) would be $336 million, with the state share approximately $140 million.

ii. Medicare
1. Lobby Congressional delegation to include eHealthTrust as Medicare benefit as "demonstration project"
2. Many Medicare recipients may elect to join on their own
3. Total Federal cost to enroll Medicare recipients in a typical state of 5 million with 700,000 beneficiaries would be $42 million/year (same as Medicaid example above). Potential annual savings would again be $336 million.

iii. Uninsured
1. In each community, the uninsured receive uncompensated care
2. Those who are providing care would save money by enrolling the uninsured in the eHealthTrust (by avoiding medical errors and duplication due to lack of information)

3. Community stakeholders should be encouraged to meet and develop a plan for enrolling the uninsured in the eHealthTrust

IX. Risks & Mitigation Strategies

a. Business risks
   i. Market risk: eHealthTrust business success depends on enough subscribers to break even
      1. Breakeven at 100,000 subscribers for Phase I represents only 2% of population in a state of 5,000,000 → very low risk
      2. Low risk can be further verified by surveying consumers in the proposed marketing area to confirm strong demand for electronic records at the proposed price point (ask consumers if they are willing to pay $5/month for their own electronic records)
      3. Commitment for immediate signup of a large initial group of subscribers nearly eliminates market risk as breakeven would be assured
   ii. Technical risk ("can the system be built?") is minimal
      1. No new technology or concepts are needed
      2. System design is simple and straightforward
   iii. Management risk is low and controllable
      1. Need capable and experienced Board of Directors representing local health care stakeholders
      2. Need capable and experienced management team and staff
         a. With appropriate compensation, many talented personnel are available (particularly for the first project of this kind)

b. Strategic risks: "Will eHealthTrust result in a community health information system that has complete information, cooperation of stakeholders, trust of the public, and is financially sustainable?"
   i. Complete information
      1. Depends on effectiveness of EHR incentives
      2. Has not been tested, so results not assured
      3. In Maine, $5,000/physician one-time incentives were effective in stimulating widespread EHR acquisition, so the level of incentives is adequate based on this single prior observation
      4. Slow EHR adoption does not interfere with financial sustainability
         a. Improves financial situation by reducing need for EHR incentive payments
      5. Adjustments can be made if initial incentive program is ineffective or does not result in sufficiently rapid EHR adoption

ii. Cooperation of stakeholders
    1. Assured with HIPAA, but may be a problem in practice
        a. HIPAA does not explicitly require electronic information to be provided
        b. Electronic information will be the easiest and lowest cost way to respond to large numbers of requests
        c. Some persuasion of stakeholders to provide electronic information may be needed
            i. Providing patient information for care is an established public policy principle
            ii. Withholding patient information (or providing it in a form that is not useful) would be very negative from a public relations perspective
            iii. If absolutely necessary, can seek state legislation
iii. Trust of the public
    1. Should be assured through
        a. Consumer representation on Board of non-profit
        b. Open and transparent management
        c. Independent privacy review committee
    2. Has not been tested, so must be monitored closely
    3. Adjust organization & policies as needed
iv. Financial sustainability (see “Business risks” above)